Probabilistic Safety Assessment – Safety & Regulatory Framework

Presentation to the CNSC
August 2017

Dr. V.G. Snell

Purpose

To summarize work done under CNSC contract 87055-16-0251:

“Role of the Probabilistic Safety Assessment (PSA) in the Safety Analysis Area and in the Regulatory Framework”

Background

"The Canadian Nuclear Safety Commission requires the services of a contractor to conduct a review and produce a report that will 1) document the regulatory role of the PSA and 2) document and provide an independent discussion of the role of the Whole–Site PSA."

Process

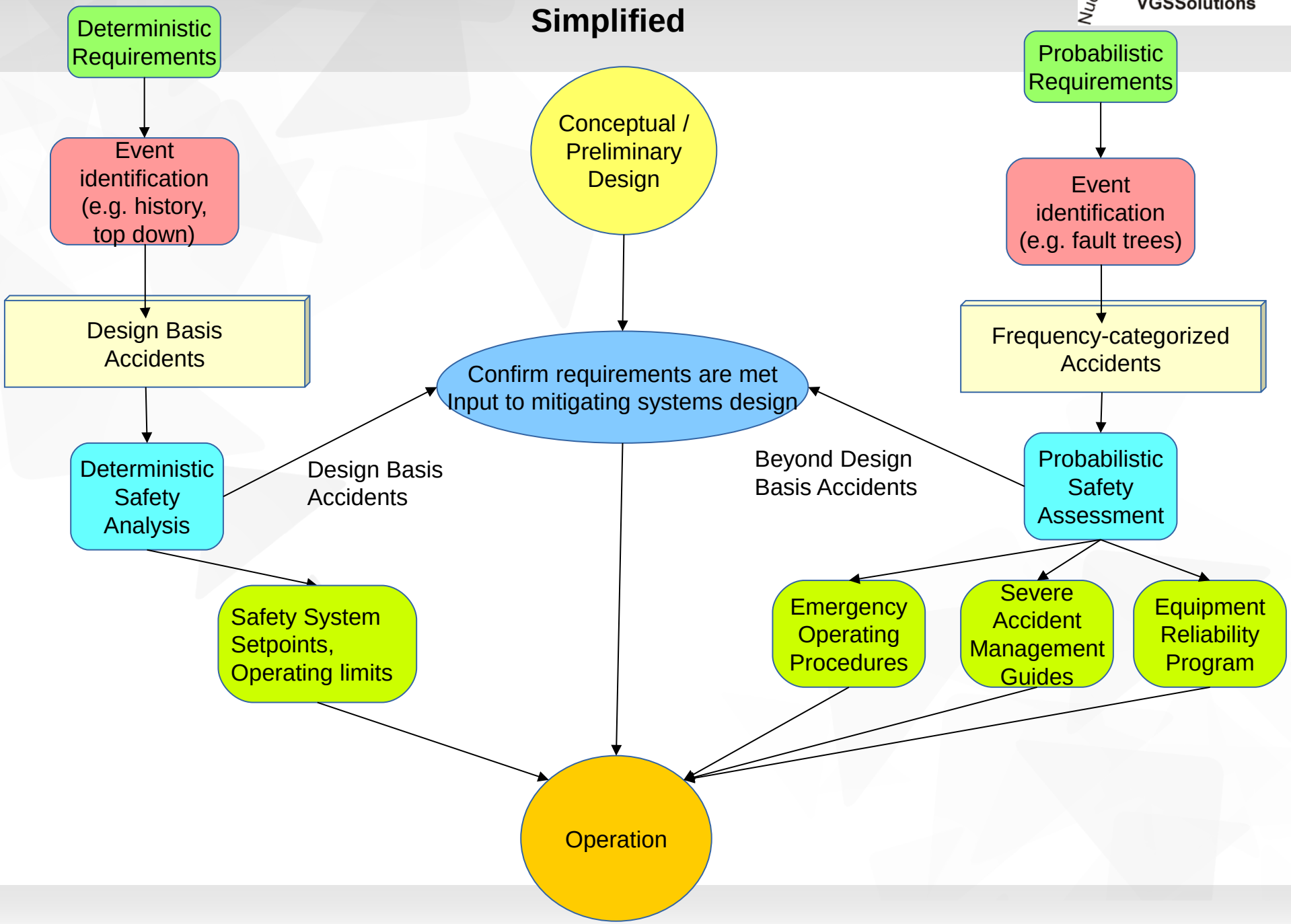
- Reviewed selected current national and international regulatory practices in Deterministic Safety Analysis (DSA) and PSA
- Used personal experience
- Analyzed the information to draw conclusions & recommendations
- Written for public audience: no protected material or references
- Independent

Safety Analysis is not the same as Safety

- Nuclear Power Plant safety depends on many factors:
  - Fundamental design characteristics
  - Standards to which equipment is designed and built
  - In-service inspection
  - Operating competence
  - Configuration control
  - Safety culture
  - Engineering knowledge of the reactor / design authority
  - Etc.
- Safety analysis – one means of testing design and operation of mitigating systems and human actions against postulated accidents

Topic 1 – Regulatory Role of PSA

Safety Analysis - Simplified



Deterministic Safety Analysis & Design Basis Accidents

- Traditional approach – based on experience in research reactors (e.g. criticality accidents) + heuristic review of “what could go wrong” in power reactors
- Select smaller set with apparently bounding consequences
- Use pessimistic assumptions to analyze them
- Use in design of mitigating systems → Design Basis Accidents (DBAs)
- Premise: If a plant could be shown analytically to withstand a set of apparently-bounding stylized accidents using pessimistic assumptions, it could therefore withstand the much larger number of accidents which might actually occur.

Probabilistic Safety Assessment

- Answers three questions:
  - What can go wrong?
  - How likely is it to happen?
  - If it happens, what are the consequences?
- US Reactor Safety Study (RSS) - 1975
  - Fault trees to determine the frequency of initiating events
  - Event trees to determine the failure frequency of mitigating systems and containment

RSS Insights

- The most severe Design Basis Accidents were not necessarily the ones that dominated risk (large vs. small Loss of Coolant Accident)
- Some event *combinations* could lead to core melt at frequencies comparable to DBAs
- Core melt sequences were more frequent than previously estimated but had lower consequences
- Human error major accident contributor

DBA/DSA – Strengths & Weaknesses

Strengths

- Pessimistic answers → “real” accidents less severe
- Safety analysis effort optimized
- Can apply early on in design process

Weaknesses

- Not useful for risk-informed decisions – event selection can be inconsistent
- Misleading for accident management procedures
- Be careful on what is conservative
- Hard to identify combined or consequential events

PSA – Strengths & Weaknesses

Nuclear Safety, Education & Licensing
VGSSolutions

Strengths

- Provides comparative risk → optimization of resources
- Very effective in early design
- Evaluates balance between automatic and operator action
- Gateway to Beyond Design Basis Accidents (BDBAs), including severe accidents
- Basis for Emergency Operating Procedures, Severe Accident Management Guides
- Identify cliff-edge effects

Weaknesses

- Does not predict absolute risk
- Characteristics of very rare single events?
- Software errors
- Subtle common-cause failures
- Fully-passive structures / systems
- Safety culture
- Malevolent acts

PSA in Operational Decision-Making

- Proposed design changes
- Impairments in safety-related equipment
- Optimized maintenance, testing, inspection
- Discovery issues

In short ...

- **PSA/DSA strengths and weaknesses complementary – both should be used**

PSA in Canada

- Long history
- NRX research reactor accident – fundamental rethinking of power reactor philosophy. Part of it:
  - Control frequency of severe accident to meet safety goal by limiting frequency of process system failures and safety system demand unavailability
- Douglas Point – risk analysis basis
  - Weakness: treatment of common cause failures
  - But gave designer & operator specific tools to measure success – world first

Large CANDU Licensing

- Shift away from probabilistic techniques
  - Single / dual failures, and later C-6
  - Still required safety system reliability → PSA techniques
- Safety Design Matrices
  - Used by designer to address weaknesses in DSA
  - Limited scope PSA
  - Designer-proposed acceptance criteria → *many* changes
  - PSAs now done for all CANDUs

Regulatory Status of PSA in Canada

- Not specified in Nuclear Safety and Control Act nor Class 1 Regulations
  - CNSC has broad discretion
- Specified in CNSC “REGDOC” and “RD” series
  - REGDOC 2.4.2 (Probabilistic Safety Analysis) - scope
  - RD/GD-369 (Licence to Construct a Nuclear Power Plant) implies it is optional (“should”)
  - REGDOC-2.5.2 (Design) uses “shall”

Recommendation 1: The next revision of Regulatory Document RD/GD-369 should be made consistent with REGDOC-2.5.2 – i.e. to state that a PSA is a requirement for a construction licence.

Non-Power Reactors

- NRU PSA summary published
- Not found anything published for other non-power reactors, but referred to
- Scope should be tailored to fit the inherent hazard and complexity of the non-power reactor

Recommendation 2: CNSC should ensure that a suitable PSA is performed at the appropriate time for non-power reactors, and a public summary made available.

Safety Goals

- CNSC Numerical Safety Goals
  - Frequency limits on core damage, small release of radioactive material, large release of radioactive material
- Showing compliance requires PSA
- Problems with pass/fail criterion – implies *incorrectly*:
  - Precision in the PSA
  - Risk changes abruptly as one crosses this boundary; and
  - Existing plants are less acceptably safe than new designs

Recommendation

Recommendation 3: CNSC should explain the meaning of its safety goals in a way which acknowledges the inherent uncertainties of both acceptable risk and the means used to calculate it.

Note: some other countries use a range of acceptability

PSA in Operations – Risk-Informed

- Plant configuration management during outages
- Event analysis
- Neutron Overpower Protection optimization
- Risk-Informed In-service Inspection
- Request for changing test/maintenance intervals
- Request for changes in Operating Policies and Principles
- Large Pipe Break reclassification

Recommendation 4: CNSC should encourage the nuclear industry to summarize publicly how PSA is used in day-to-day operation.

Comparison to International Practice - 1

	Require Numer-ical Safety Goals	*PSA Required in Pre-Project Design*	*PSA Required for Construct-ion Licence*	*PSA Required for Operating Licence*	*PSA Required for Periodic Safety Review*	*PSA Used for Technical Specific-ations etc.*	*PSA Used to Risk-Inform Regula-tions*
Canada	√	Vendor Design Review	√	√	√	√	√
United Kingdom	√	√	√	√	√	√	√
United States	Guide	Design Certifica-tion	-	-	-	√	√
Finland	√	-	√	√	√	√	√
Argentina	√	-	√	√	√	√	√
France	-	-	-	-	√	√	√
Germany	-	-	-	-	√	√	√

Comparison to International Practice - 2

- Indicative, not exhaustive survey of all countries
- All countries sampled use PSA to risk-inform their regulatory approach
- The US, France and Germany do not give PSA a formal role in regulation of existing plants
- PSA is used in formal regulation in Canada, the U.K., Argentina and Finland
- The U.K. emphasizes the process for a design-phase PSA even prior to a licence application (i.e. as part of the management system for the project)

Topic 1 Conclusion: Canada is generally consistent with best world practices in the way it uses PSA in regulation

Topic 2 – Whole-Site PSA

Overview

- Multi-unit sites pose obvious challenge
  - To date PSAs are based on single-units with some incomplete treatment of multi-unit effects
  - In Ontario, plants share parts of safety systems (containment, Emergency Core Cooling, emergency electrical power & water)
- Multiplying single-unit PSA numbers by the number of units could be quite wrong
  - Overestimates risk because some common-cause events are already included in the single-unit PSA
  - Underestimates risk because it does not look explicitly at all multi-unit effects
- Other sources of radioactive material – spent fuel bays

Broader Whole-Site Issues

- Off-site effects which could impact the events on the nuclear plant site
- Unexpected interactions among plant components
- Unexpected interactions among nuclear units
- Unexpected adverse conditions on-site (e.g. radiation, debris, lack of communication, organizational failure)
- Cliff-edge effects
- Appropriate mission time for mitigating measures and equipment
- Human performance in multi-unit events
- The difficulty of estimating the probability of rare destructive external events, leading to premature “screening out” from consideration

The Seabrook Multi-Unit PSA (1983)

- Despite the limited sharing, the frequency of core damage (CDF) to both units was close to 10% of the frequency of damage to one unit

Risk Metric	Mean Value
Single Reactor Unit CDF	2.3×10^{-4}/reactor-year
Two Unit Station CDF	
- Core damage to one reactor	4.0×10^{-4}/station-year
- Core damage to both reactors	3.2×10^{-5}/station-year
- Total	4.3×10^{-4}/station-year

Multi-Unit Techniques

- Whole Site PSA
  - Same strengths and weaknesses as single-unit PSA
  - No reason it can't be done
  - Pilot Whole-Site PSA started by the Canadian Nuclear Industry
  - Level 3 Whole-Site PSA started by USNRC
  - Others starting or have started:
    - Europe: Advanced Safety Assessment Methodologies: Extended PSA
    - International Atomic Energy Agency (IAEA): Information sharing

Other non-PSA Techniques

- Emergency Mitigating Equipment (Canada)
- Diverse and Flexible Coping Strategies (US)
- Threat-risk assessment (from security industry)
- Fault-sequence analysis (stress tests) (IAEA)

Advantages of Whole-Site PSA

- Systematic way of revealing vulnerabilities
- Accurate health effects
- Physical insight into accident mechanisms and inter-dependencies
- Allows analyses of the risk-effectiveness of mitigation strategies

Results only as good as the data
Continuing role for deterministic approaches

Recommendations - 1

- Recommendation 5: In principle Whole Site PSA offers insights that deterministic methods cannot. This will be confirmed by the pilot Whole Site PSA being performed by the Canadian nuclear industry for Pickering. We recommend that incorporation of Whole Site PSA into the regulatory framework await the results of this pilot project: if the insights were worth the effort, it would be logical to build regulatory requirements around it. Specifically we recommend that debates about whole-site safety goals do not need to be resolved until the pilot project has been completed. While it is customary to set requirements before embarking on analyses, we believe that for a pilot study, the requirements will be informed by the results, in terms of what is practicable and in terms of the uncertainties in the methodology.

Recommendations - 2

Recommendation 6: Since the usefulness of a Whole Site PSA depends strongly on the quality of the methodology, we encourage early informal interaction between the CNSC and the Canadian nuclear industry on the methodology proposed.

Multi-Unit PSA

Topic 2 Conclusion: At present, Canada leads the world in potential application of Whole Site PSA, based on the pilot project for Pickering being performed by the Canadian nuclear industry, and assuming it is completed in a timely manner.

Overall Summary

- Deterministic and Probabilistic Safety Analyses are complementary and equally important. Canada is consistent with best practices in the use of PSA in regulation
- The application of Whole-Site PSA to Pickering is a useful extension of PSA and will give valuable insights into the safety of multi-unit sites.